UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF PENNSYLVANIA

MARK DUSHOK, GUARDIANS/ PARENTS A.F. AND G.G-F. ON BEHALF OF MINOR PLAINTIFFS A.G-F AND K.G-F., GUARDIAN/ PARENT CHRISTINA IZQUIERDO ON BEHALF OF MINOR PLAINTIFF X.T., individually and on behalf of all others similarly situated, Plaintiffs, v. **NUANCE COMMUNICATIONS, INC. and GEISINGER HEALTH d/b/a GEISINGER HEALTH FOUNDATION,** Defendants.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Mark Dushok, minors A.G-F and K.G-F through their guardians/parents A.F. and G.G-F., and Plaintiff Christina Izquierdo, individually and as a guardian/parent on behalf of minor Plaintiff X.T. (where necessary to protect the identities of the minors, guardians/parents are referred to by initials) (collectively referred to herein as "Plaintiffs"), bring this Class Action Complaint, individually and on behalf of themselves and on behalf of all others similarly situated (the "Class Members"), against Defendants Nuance Communications, Inc. ("Nuance") and Geisinger Health d/b/a Geisinger Health Foundation ("GH")

(Geisinger and Nuance are jointly referred to herein as "Defendants"), alleging as follows, based upon information and belief, investigation of counsel, and personal knowledge of Plaintiffs.

INTRODUCTION

1. Plaintiffs bring this class action lawsuit against Defendants for failure to properly secure and safeguard Plaintiffs and Class Members' personally identifiable information ("PII") and protected health information ("PHI," and collectively with PII, "Private Information") including dates of birth, addresses, admit, discharge and transfer codes, medical record numbers, race, gender, phone numbers and facility name abbreviations.

2. Nuance is a computer software technology corporation based out of Burlington, Massachusetts. Nuance is an IT vendor of GH, which is a regional health care provider headquartered in Danville, Pennsylvania.

3. On or around November 29, 2023, GH discovered that a former Nuance employee had accessed certain Geisinger patient information two days after the employee had been terminated. Following an investigation, Nuance determined that more than one million GH patients were impacted by the data breach (the "Data Breach"). Nuance, on behalf of GH, began sending out notice letters to individuals impacted on June 21, 2024.

4. Despite its vast experience as a healthcare provider, GH did not protect the

Private Information of their patients—the Class Members.[1]

5. Despite its vast experience as a computer software technology company and IT vendor[2], Nuance did not protect the Private Information of their client GH's patients.

6. Defendants had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on their affirmative representations to Plaintiffs and the Class, to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

7. Defendants failed to take precautions designed to keep patients' Private Information secure.

8. Defendants owed Plaintiffs and Class Members a duty to take all reasonable and necessary measures to keep the Private Information collected safe and secure from unauthorized access. Defendants solicited, collected, used, and derived a benefit from the Private Information, yet breached its duty by failing to implement or maintain adequate security practices.

9. The sensitive nature of the data exposed through the Data Breach signifies

[1] "Private Information" contains information such as names, physical addresses, phone numbers, dates of birth, health insurance account information, Social Security numbers, provider taxpayer identification numbers, and clinical information (e.g., medical history, diagnoses, treatment, dates of service, and provider names).

[2] *See* https://www.nuance.com/index.html.

that Plaintiffs and Class Members have suffered irreparable harm. Plaintiffs and Class Members have lost the ability to control their Private Information and are subject to an increased risk of identity theft.

10. Defendants, despite having the financial wherewithal and personnel necessary to prevent the Data Breach, nevertheless failed to use reasonable security procedures and practices appropriate to the nature of the sensitive information maintained, causing the exposure of Private Information for Plaintiffs and Class Members.

11. Even if stolen PII or PHI does not include financial or credit card payment account information, that does not mean there has been no harm to the victims of the breach, or that the breach does not cause a substantial risk of identity theft. Freshly stolen Private Information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained Private Information about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

12. Based on the value of its patients' Private Information to cybercriminals, Defendants knew or should have known the importance of safeguarding the Private Information entrusted to it and of the foreseeable consequences if its data security

systems were breached. Defendants failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

13. Defendants maintained Class Members' Private Information in a negligent and/or reckless manner. In particular, the Private Information was maintained on Defendant GH's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendants, and as such Defendants were on notice that failing to take steps necessary to secure Private Information from those risks left that Private Information in a vulnerable condition.

14. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial accounts and taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' Private Information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, and giving false information to police during an arrest.

15. As a result of the Data Breach and exposure of their Private Information online, Plaintiffs and Class Members face a substantial risk of imminent and

certainly impending harm. Plaintiffs and Class Members have and will continue to suffer injuries associated with this risk, including but not limited to a loss of time, mitigation expenses, and anxiety over the misuse of their Private Information.

16. As a result of the Defendants' inadequate digital security, Plaintiffs' and Class Members' Private Information was accessed by an unauthorized third party. Plaintiffs and Class Members have suffered and will continue to suffer injuries including financial losses caused by misuse of Private Information; the loss or diminished value of their Private Information as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of personal and medical information.

17. Even those Class Members who have yet to experience identity theft have to spend time responding to the Data Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiffs and Class Members have incurred, and will continue to incur, damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, diminished value of Private Information, loss of privacy, and/or additional damages as described below.

18. Accordingly, Plaintiffs bring this action against Defendant seeking redress for their unlawful conduct and asserting claims for: (i) negligence; (ii) negligence

per se; (iii) breach of implied contract; and (iv) unjust enrichment. Through these claims, Plaintiffs seeks damages in an amount to be proven at trial, as well as injunctive and other equitable relief, including improvements to Defendants' data security systems and controls, future annual audits, and adequate credit monitoring services funded by Defendants.

THE PARTIES

Plaintiffs

19. Plaintiff Mark Dushok ("Dushok") is a citizen of Pennsylvania and resides in Duryea, Pennsylvania, in the County of Luzerne. Plaintiff Dushok is a patient of Geisinger Health. On June 21, 2024 Nuance sent Plaintiff Dushok a notice letter informing him that he was impacted by the Data Breach. As a result of the Data Breach, Plaintiff Dushok has experienced an uptick in spam calls, texts, and emails. Further, Experian has advised Plaintiff Dushok that his data has been found on "suspicious websites." As an additional result of the Data Breach, Plaintiff Dushok has been forced to, and will continue to, invest significant time monitoring his accounts to detect and reduce the consequences of likely identity fraud. As a result of the Data Breach, Plaintiff Dushok is now subject to substantial and imminent risk of future harm. Had Plaintiff Dushok known that Defendants do not adequately protect the Private Information in their Possession, Plaintiff Dushok would not have agreed to provide Defendants with his Private Information or obtained healthcare

services from GH.

20. Plaintiffs are minors named A.G-F. and K.G-F., and their guardians/parents A.F. and G.G-F. (where necessary to protect the identities of the minors, guardians/parents are referred to by initials) are, and at all relevant times have been, residents and citizens of Clarks Summit, Pennsylvania in the County of Lackawanna. A.F. and G.G-F., individually and on behalf of minor Plaintiffs A.G-F and K.G-F., are patients of Geisinger Health. On June 21, 2024, Nuance sent minor Plaintiffs A.G-F. and K.G-F., each notice letters informing them that they were impacted by the Data Breach. As a result of the Data Breach, A.F. and G.G-F., on behalf of minor Plaintiffs A.G-F. and K.G-F. have experienced an uptick in spam calls, texts, and emails. As an additional result of the Data Breach, A.F. and G.G-F., on behalf of minor Plaintiffs A.G-F. and K.G-F. have been forced to, and will continue to, invest significant time monitoring their accounts to detect and reduce the consequences of likely identity fraud. Also, as a result of the Data Breach, A.F. and G.G-F., on behalf of minor Plaintiffs A.G-F. and K.G-F. are now subject to substantial and imminent risk of future harm. Had A.F. and G.G-F., on behalf of minor Plaintiffs A.G-F. and K.G-F. known that Defendants do not adequately protect the Private Information in their Possession, A.F. and G.G-F., individually, and on behalf of minor Plaintiffs A.G-F. and K.G-F. would not have agreed to provide Defendants with their Private Information or obtained healthcare services from GH.

21. Plaintiff is a minor named X.T. and his/her guardian/parent Christina Izquierdo ("Ms. Izquierdo") are, and at all relevant times have been, residents and citizens of Scranton, Pennsylvania in the County of Lackawanna. Ms. Izquierdo, individually and on behalf of minor Plaintiff X.T., are patients of Geisinger Health. On June 21, 2024, Nuance sent Ms. Izquierdo, and minor Plaintiff X.T. each notice letters informing them that they were impacted by the Data Breach. As a result of the Data Breach, Ms. Izquierdo, individually and on behalf of minor Plaintiff X.T. has experienced an uptick in spam calls, texts, and emails. Further, Experian has advised Plaintiff Ms. Izquierdo that her data has been found on "suspicious websites." As an additional result of the Data Breach, Ms. Izquierdo, individually, and on behalf of minor Plaintiff X.T. has been forced to, and will continue to, invest significant time monitoring their accounts to detect and reduce the consequences of likely identity fraud. Also, as a result of the Data Breach, Ms. Izquierdo, individually, and on behalf of minor Plaintiff X.T., are now subject to substantial and imminent risk of future harm. Had Ms. Izquierdo, individually, and on behalf of minor Plaintiff X.T. known that Defendants do not adequately protect the Private Information in their Possession, Ms. Izquierdo, individually, and on behalf of minor Plaintiff X.T. would not have agreed to provide Defendants with their Private Information or obtained healthcare services from GH.

22. To obtain healthcare services from Defendant GH, Plaintiffs provided

Defendant GH with highly-sensitive Private Information—including financial and health information—which was then stored on GH's systems and maintained and accessed by Defendants.

23. Defendants obtained and continue to maintain the Private Information of Plaintiffs and owed them a legal duty and obligation to protect their Private Information from unauthorized access and disclosure. Plaintiffs' Private Information was compromised and disclosed because of Defendants' inadequate data security, which resulted in the Data Breach.

24. Defendant Nuance's Notice explained the importance of protecting Private Information, and steps that Plaintiffs should take to ensure the safety of her Private Information as a result of the Data Breach (Notice Attachment "Additional Steps You Can Take"). Accordingly, Plaintiffs spent time monitoring their credit reports and accounts, researching identity theft and protection options, and researched additional steps that they should take to protect themselves as a result of Defendants' wrongdoing.

25. As a result of the Data Breach, Plaintiffs have experienced increased concerns, anxiety and emotional distress over the loss of privacy they experienced because of the Data Breach.

26. Further, Plaintiffs have experienced anxiety and emotional distress given the increased likelihood of harm they or their minor children have been exposed to

because of Defendants' wrongdoing. Plaintiffs have suffered imminent and impending injury arising from the substantially increased likelihood of fraud, identity theft, and misuse of their Private Information being compromised and placed in the hands of third-party criminals.

27. Importantly, criminals steal Private Information for a reason: to misuse it later. Plaintiffs' Private Information was targeted for the purpose of committing fraud. Accordingly, Plaintiffs have an ongoing interest in ensuring that their information is not used for nefarious purposes.

Defendants

28. Defendant Nuance Communications, Inc. is a Delaware corporation with its principal place of business located in Burlington, Massachusetts. Nuance is a provider of computer software technology.

29. Defendant Geisinger Health d/b/a Geisinger Health Foundation is a Pennsylvania corporation headquartered in Danville, Pennsylvania. Geisinger is a regional health care provider to central, south-central and northeastern Pennsylvania.

JURISDICTION AND VENUE

30. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because at least one member of the putative Class, as defined below, is a citizen of a different state than Defendant, there are

more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

31. This Court has personal jurisdiction over Defendant GH because Defendant Geisinger is registered to do business in, and maintains its principal place of business in Danville, Pennsylvania.

32. The Court has specific personal jurisdiction over Defendant Nuance because Nuance purposely availed itself of the laws of Pennsylvania by acting as a vendor to GH that provides it with information technology services.

33. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(2) because Defendant Geisinger's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to the Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

34. Geisinger's business is to focus on the wellbeing and health of its patients; its collaboration places a great deal of emphasis on guaranteeing that it knows how to best care for its patients; however, in spite of these promises, Geisinger failed to take sufficient steps to guarantee the privacy and security of Private Information.

35. Upon information and belief, Defendants made promises and representations to consumers and patients, including Plaintiffs and Class Members, that the Private Information collected from them would be kept safe, confidential,

and that the privacy of that information would be maintained.

36. Plaintiffs and Class Members provided their Private Information to Defendants with the reasonable expectation and on the mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

37. As a result of collecting and storing the Private Information of Plaintiffs and Class Members for their own financial benefit, Defendants had a continuous duty to adopt and employ reasonable measures to protect Plaintiffs and the Class Members' Private Information from disclosure to third parties.

38. To obtain healthcare services, patients, like Plaintiffs and Class Members, must provide their doctors, medical professionals, and administrators working for or with Defendants directly with highly sensitive private information. As part of their regular and ordinary course of business, Defendants Geisinger and Nuance then compile, store, and/or maintain the Private Information they receive from patients.

39. Because of the highly sensitive and personal nature of the information Defendants acquired and stored with respect to patients and other individuals, Defendants, upon information and belief, promised to (among other things): keep PHI private; comply with health care industry standards related to data security and Private Information, including HIPAA; inform consumers of their legal duties and comply with all federal and state laws protecting consumer Private Information; only

use and release Private Information for reasons that relate to medical care and treatment; and provide adequate notice to individuals if their Private Information is disclosed without authorization.

40. As a HIPAA-covered business entity, Defendant GH is required to implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured PHI as in the case of the Data Breach complained of herein.

41. However, Defendant GH did not maintain adequate security to protect its systems from infiltration by cybercriminals.

42. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

43. Defendants were in the best position to safeguard the most sensitive information it obtained from Plaintiffs and Class Members. Their unique position enabled GH and Nuance to collect and maintain some of the most sensitive information on Plaintiffs and Class Members; accordingly, Defendants had a special relationship with Plaintiffs and Class Members such that they should have

safeguarded that data.

44. These data security and privacy promises were not kept; Defendants experienced a massive data breach and have not even provided information about how long the data breach existed before it was detected, much less an accurate picture of how many patients were implicated in the data breach.

Geisinger Health Is Subject to HIPAA

45. Defendant Geisinger is a HIPAA covered entity that provides services to patients and healthcare and medical service providers. As a regular and necessary part of its business, Defendant GH collects the highly sensitive Private Information of its own patients and its clients' patients and Defendant Nuance had access to that highly sensitive Private Information of the patients and clients.

46. As a HIPAA covered entity, Defendant Geisinger is required under federal and state law to maintain the strictest confidentiality of the patient's Private Information they acquire, receive, and collect, and Defendants Geisinger and Nuance are further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

47. As a HIPAA covered entity, Defendant Geisinger is required to implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information. This

includes incidents that constitute breaches of unsecured PHI as in the case of the Data Breach complained of herein.

48. Defendant GH is in the business of providing a range of healthcare services to patients – which necessarily includes storing and maintaining electronic health records. Defendant GH would be unable to engage in its regular business activities without collecting and aggregating Private Information that it knows and understands to be sensitive and confidential. In the ordinary course of Defendants' businesses, Defendant Nuance had complete access to Defendant GH's electronic records containing the Plaintiffs' and the Class Members' Private Information.

49. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

50. Plaintiffs and Class Members are or were patients whose medical records and Private Information were maintained by Defendants and/or its affiliated hospital campuses, care sites, and other medical providers, who received health-related or other services from Defendant GH, and/or individuals who directly or indirectly entrusted Defendants with their Private Information.

51. Plaintiffs and the Class Members relied on Defendants to implement and follow adequate data security policies and protocols, to keep their Private

Information confidential and securely maintained, to use such Private Information solely for business and health care purposes, and to prevent the unauthorized disclosures of their Private Information. Plaintiffs and Class Members reasonably expected that Defendants would safeguard their highly sensitive information and keep that Private Information confidential.

52. As described throughout this Complaint, Defendants did not reasonably protect, secure, or store Plaintiffs' and Class Members' Private Information prior to, during, or after the Data Breach, but rather, enacted unreasonable data security measures that they knew or should have known were insufficient to reasonably protect the highly sensitive information Defendants stored and maintained. Consequently, cybercriminals circumvented Defendants' security measures, resulting in a significant Data Breach.

The Geisinger Health Data Breach and Notice Letter

53. As a HIPAA covered business entity that collects, creates, and maintains significant volumes of Private Information, the targeted attack was a foreseeable risk which Defendants GH and Nuance were aware of and knew they each had a duty to guard against. This is particularly true because the targeted attack appears to have been by a *former employee of Defendant Nuance.* It is well-known that healthcare businesses and insurers such as Defendant GH, which collects and stores the confidential and sensitive PII/PHI of over a million individuals, and Defendant

Nuance, which provides information technology services to GH and has access to and maintains the confidential and sensitive PII/PHI of over a million individuals, are frequently targeted by cyberattacks. Further, cyberattacks are highly preventable through the implementation of reasonable and adequate cybersecurity safeguards, including proper employee cybersecurity training and proper procedures governing former employees.

54. The targeted cyberattack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients, like Plaintiffs and Class Members.

55. Defendant Geisinger had obligations created by HIPAA, contract, industry standards, common law, and its own promises and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure. Defendant Nuance had obligations created by its complete access to the Private Information maintained and stored by Defendant GH.

56. Plaintiffs and Class Members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

57. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and

Class Members' Private Information, Defendants assumed legal and equitable duties and knew, or should have known, that they were responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

58. Due to Defendants' inadequate security measures and their woefully inadequate notice to victims, Plaintiffs and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft that they will have to deal with for the rest of their lives.

Geisinger Health was on Notice to the Foreseeable Risk of a Data Breach

59. As a HIPAA covered entity handling the medical patient data of insureds, Defendants data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry, and other industries holding significant amounts of PII and PHI, preceding the date of the breach.

60. At all relevant times, Defendants knew, or should have known that Plaintiffs' and Class Members' Private Information was a target for malicious actors. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class Members' Private Information from cyberattacks that Defendant should have anticipated and guarded against.

61. Moreover, Defendants failed to implement and maintain reasonable and

appropriate data privacy and security measures that would timely alert Defendants of any such attack, should one occur.

62. In light of recent high profile data breaches at other health care providers, Defendants knew or should have known that their electronic records and consumers' Private Information would be targeted by cybercriminals and ransomware attack groups.

63. The rate of healthcare data breaches has been on the rise in the past six years. "In 2018, healthcare data breaches of 500 or more records were being reported at a rate of around 1 per day. Fast forward 5 years and the rate has more than doubled. In 2022, an average of 1.94 healthcare data breaches of 500 or more records were reported each day."[3]

64. Cyber criminals seek out PHI at a greater rate than other sources of private information. In a 2022 report, the healthcare compliance company, Protenus, found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[4]

65. In light of recent high profile cybersecurity incidents at other healthcare

[3] *See Healthcare Data Breach Statistics,* HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last viewed July 17, 2024).

[4] *See 2022 Breach Barometer*, PROTENUS, https://blog.protenus.com/key-takeaways-from-the-2022-breach-barometer (2022) (last viewed July 17, 2024).

partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that their electronic records would be targeted by cybercriminals.

66. Indeed, cyberattacks against the healthcare industry have been common for over eleven years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[5]

67. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[6] A cybercriminal who steals a person's PHI can end up with as many as

[5] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://financialservices.house.gov/uploadedfiles/091411snow.pdf.

[6] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (stating "Health information is a treasure trove for criminals.").

"seven to 10 personal identifying characteristics of an individual."[7] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident in 2010, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[8]

68. Cyberattacks on medical systems, like Defendant GH's, have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[9]

69. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year.

---

[7] *Id.*
[8] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/.
[9] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

Almost three-quarters of those breaches were classified as hacking/IT incidents."[10]

70. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[11] In this case, Defendant stored the records of *millions* of patients.

71. Private Information, like that stolen from Defendants, is "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[12]

72. Cybercriminals also maintain encrypted information on individuals to sell in "fullz"[13] records because that information can be foreseeably decrypted in the

[10] The HIPAA Journal, *Editorial: Why Do Criminals Target Medical Records* (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records.
[11] *See id.*
[12] *See id*.
[13] *See* Investopedia "Fullz (or "fulls") is a slang term for "full information." Criminals who steal credit card information use the term to refer to a complete set of information on a prospective fraud victim. https://www.investopedia.com/fullz-definition-4684000.

future.

73. Given these facts, any company that transacts business with consumers – and medical patients -- and then compromises the privacy of consumers' Private Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

74. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[14]

75. Defendant were on notice that the FBI has concerns about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[15]

76. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential

[14] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack, Security Magazine* (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

[15] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare- firms-they-are-targeted-by-hackers-idINKBN0GK24U20140820.

information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[16]

77. As implied by the above AMA quote – "patient access to care" -- stolen Private Information can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiffs and Class Members.

78. The U.S. Department of Health and Human Services and the Office of Consumer Rights ("OCR") urges the use of encryption of data containing sensitive private information. As far back as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive private information. In announcing the fines, Susan McAndrew, formerly OCR's deputy director of health information privacy, stated in 2014 that "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[17]

---

[16] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED.ASS'N (Oct 4, 2019), https://www.ama-assn.org/practice-anagement/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals.

[17] Susan D. Hall, *OCR levies $2 million in HIPAA fines for stolen laptops*, Fierce Healthcare (Apr. 23, 2014), https://www.fiercehealthcare.com/it/ocr-levies-2-million-hipaa-fines-for-stolen- laptops.

79. As a HIPAA covered entity and its information technology vendor, Defendants should have known about their data security vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the Private Information stored in their unprotected files.

Geisinger Health Failed to Comply with FTC Guidelines

80. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should factor into all business decision-making.

81. In 2016, the FTC updated its publication, Protecting Private Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of private information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[18] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity

[18] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (Oct. 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf- 0136_proteting-personal-information.pdf.

indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and, have a response plan ready in the event of a breach.[19]

82. The FTC further recommends that companies not maintain PII longer than necessary for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

83. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

84. These FTC enforcement actions include actions against healthcare providers and partners like Defendant. *See*, *e.g.*, *In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were

[19] *Id.*

unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

85. Defendants failed to properly implement basic data security practices, including by failing to implement an adequate intrusion detection system which would expose a breach as soon as it occurs.

86. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

87. Defendants were at all times fully aware of its obligations to protect the Private Information of customers and patients. Defendants were also aware of the significant repercussions that would result from their failures to do so.

Geisinger Health Failed to Comply with Industry Standards

88. As described above, experts studying cybersecurity routinely identify healthcare providers and partners as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

89. Several best practices have been identified that at a minimum should be implemented by healthcare service providers like Defendant GH and its information technology vendor, Defendant Nuance, including but not limited to; educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key;

multi-factor authentication; backup data; and limiting which employees can access sensitive data.

90. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

91. On information and belief, Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

92. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendants failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

Geisinger's Conduct Violates HIPAA Obligations to Safeguard PII and PHI

93. As a healthcare company, and by handling medical patient data, Defendant GH is, and acknowledges that it is, a covered entity under HIPAA (45 C.F.R. § 160.103) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C. HIPAA covered entity Defendant Geisinger's information technology vendor Defendant Nuance – which has complete access to GH's patient data, is also subject to the HIPAA rules and regulations.

94. HIPAA requires a covered entity to protect against reasonably anticipated threats to the security of sensitive patient health information.

95. Defendants are subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

96. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information that is kept or transferred in electronic form.

97. HIPAA covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical,

technical, and administrative components.

98. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

99. A Data Breach such as the one Defendants experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI."

See 45 C.F.R. 164.40.

100. The Data Breach resulted from a combination of insufficiencies that demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations.

Consumers Are Subject to an Increased Risk of Fraud and Identity Theft as a Result of Cyberattacks and Data Breaches

101. Cyberattacks and data breaches at health care companies like Defendant GH and its information technology vendor Defendant Nuance are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

102. Researchers have found that among medical service providers that experience a data security incident, the cardiac death rate among patients increased in the months and years after the attack.[20]

103. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[21]

104. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft face "substantial costs and time to repair the damage to their good name and credit record."[22]

---

[20] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data- breaches-linked-to-uptick-in-fatal-heart-attacks.

[21] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019), https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

[22] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data

105. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal PII is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or private information through means such as spam phone calls and text messages or phishing emails.

106. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports,

---

Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[23]

107. Identity thieves use stolen Private Information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

108. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's private information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

109. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.[24]

110. Its value is axiomatic, considering the value of "big data" in corporate

---

[23] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited July 17, 2024).

[24] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

111. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered and also between when Private Information and/or financial information is stolen and when it is used.

112. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

113. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black- market" for years.

114. Stolen information has been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

115. Thus, Plaintiffs and Class Members must vigilantly monitor their financial

and medical accounts for many years to come—as Defendants have suggested that they do.

116. Private Information can sell for as much as $363 per record according to the Infosec Institute.[25] Private Information is particularly valuable because criminals can use it to target victims with frauds and scams. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

117. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[26] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[27] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

---

[25] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market.
[26] *Identity Theft and Your Social Security Number*, Social Security Administration (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.
[27] *Id.*

118. Moreover, it is no simple process to change or cancel a stolen Social Security number.

119. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even after the individual has completed the paperwork and abolished the misuse, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[28]

120. This data, as one would expect, demands a much higher price on the black market.

121. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[29]

122. Medical information is especially valuable to identity thieves.

123. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with

---

[28] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has- millions-worrying-about-identity-theft.

[29] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack- personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[30]

124. Legitimate companies buy PII on illegal or shadow markets in an attempt to increase their market share. Pharmaceutical makers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers do purchase PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Additionally, Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

125. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

126. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendant failed to properly prepare for that risk.

[30] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

Geisinger and Nuance Breached Their Obligations to Plaintiffs and Class Members

127. Defendants breached their obligations to Plaintiffs and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions based upon information and belief:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' and customers' Private Information;

c. Failing to properly monitor their own data security systems for existing intrusions;

d. Failing to ensure that vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train their employees in the proper handling of files, systems and data containing Private Information and maintain adequate email security practices;

f. Failing to ensure the confidentiality and integrity of electronic PHI they created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

k. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

l. Failing to ensure compliance with HIPAA security standard

rules by their workforces in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of their workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); Failing to render the electronic Private Information they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

n. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

o. Failing to adhere to industry standards for cybersecurity as discussed above; and

p. Otherwise breaching their duties and obligations to protect Plaintiffs' and Class Members' Private Information.

128. Defendants negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access their computer network and systems, which contained Private Information.

129. Accordingly, as set out in detail herein, Plaintiffs and Class Members are exposed to an increased risk of fraud and identity theft. And further, Plaintiffs and the Class Members also lost the benefit of the bargain they made with Defendant for health services.

Plaintiffs and Class Members' Damages

130. Due to the heightened sensitivity of the Private Information accessed during this Data Breach, Plaintiffs and Class Members have all suffered damages and will face a substantial risk of additional injuries for years to come, if not for the rest of their lives. Beyond providing inadequate credit monitoring and identify protection services, Defendants have done nothing to compensate Plaintiffs or Class Members for many of the injuries they have already suffered. Defendants have not demonstrated any efforts to prevent additional harm from befalling Plaintiffs and Class Members as a result of the Data Breach.

131. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

132. Plaintiffs' and Class Members' Private Information was all compromised in the Data Breach and are now in the hands of the cybercriminals who accessed

Defendants' computer systems.

133. In short, once PII and PHI are exposed, there is no way to ensure that the exposed data has been fully recovered or gathered and protected against future misdeeds. Because of this, Plaintiffs and Class Members will need to maintain the heightened security and monitoring measures for years, and likely for the rest of their lives due to Defendants' failures. Moreover, the value of Plaintiffs and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

134. Since being notified of the Data Breach, Plaintiffs have spent time dealing with the impact of the Data Breach, valuable time Plaintiffs otherwise would have spent on other activities, including but not limited to work, family and/or recreation.

135. Due to the Data Breach, Plaintiffs anticipate that they will need to spend considerable time and money on a regular and ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring their accounts for suspicious and/or fraudulent activity.

136. Plaintiffs' and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

137. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

138. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have been forced to spend time dealing with the effects of the Data Breach.

139. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, insurance coverage taken out in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

140. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on Plaintiffs' and Class Members' Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

141. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, and similar costs directly or indirectly related to the Data Breach.

142. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

143. Plaintiffs and Class Members were also damaged by benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service—healthcare—that was intended to be accompanied by adequate data security that complied with

industry standards, but it was not. Part of the price Plaintiffs and Class Members paid to Defendants was intended to be used by Defendants to fund adequate security of tehri computer system(s) and Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and Class Members did not get what they paid for and agreed to.

144. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time monitoring their accounts and sensitive information for misuse.

145. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent credit, banking or insurance inquiries;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Numbers, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

146. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of the Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

147. Further, as a result of Defendants' conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental, and what medications they may use—may be disclosed to the entire world, thereby subjecting them to criticism, judgment and/or embarrassment and depriving them of any right to privacy whatsoever.

148. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered anxiety, emotional distress, loss of time, loss of privacy, and are at an increased risk of future harm.

CLASS ACTION ALLEGATIONS

149. Plaintiffs bring this action against Defendants on behalf of themselves, individually, on behalf of the minor Plaintiffs, and on behalf of all other persons similarly situated ("the Class"), pursuant to Rule 23 of the Federal Rules of Civil Procedure.

150. Plaintiffs seek to represent a class of persons to be defined as follows, and proposes the following Class definition, subject to amendment as appropriate:

> **All persons in the United States and its territories who Defendants identified as being among those individuals impacted by the Data Breach announced by Nuance on or about June 2024, including all persons who were sent a notice of the Data Breach (the "Class").**

151. Excluded from the Class are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of the Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

152. This proposed class definition is based on the information available to Plaintiffs at this time.

153. Plaintiffs reserve the right to amend or modify the Class definition or create additional subclasses in an amended pleading or when she moves for class certification, as necessary to account for any newly learned or changed facts as the

situation develops and discovery proceeds and as this case progresses.

154. ***Numerosity (Rule 23(a)(1)).*** Plaintiffs are informed and believe, and thereon allege, that there are at a minimum a million members of the Class as described above. The exact size of the Class and the identities of the individual members are identifiable through Geisinger's records, including the files implicated in the Data Breach. The Members of the Class are so numerous that joinder of all of them is impracticable. Defendants acknowledged publicly that GH maintains the PII of at least 1.2 million Class Members that was compromised in the Data Breach.

155. ***Predominant Common Questions (Rule 23(a)(2)).*** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during

the Data Breach complied with applicable data security laws and regulations including, e.g., HIPAA;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendants owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendants breached their duty to Class Members to safeguard their Private Information;

g. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

h. Whether Defendants exercised reasonable diligence in their monitoring and Defendants should have discovered the Data Breach sooner;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

j. Whether Defendants' conduct was negligent;

k. Whether Defendants breached implied contracts with Plaintiffs and Class Members;

l. Whether Defendants were unjustly enriched by unlawfully

retaining a benefit conferred upon them by Plaintiffs and Class Members;

m. Whether Defendants failed to provide notice of the Data Breach in a timely

manner, and;

n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

156. ***Typicality (Rule 23(a)(3))***. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach and the claims of Plaintiffs and the Class Members are based on the same legal theories and arise from the same unlawful and willful conduct.

157. ***Adequacy of Representation (Rule 23(a)(4))***. Plaintiffs are each adequate representatives of the Class because their interests do not conflict with the interests of the Members of the Class. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs have retained Counsel who are competent and experienced in litigating class actions.

158. ***Predominance***. Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members, similar or identical violations, business

practices, and injuries are involved. Further, all the data of Plaintiffs and Class Members was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

159. ***Superiority***. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, to conduct this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

160. ***Declaratory and Injunctive Relief Appropriate.*** Defendants have acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-

wide basis.

161. Likewise, particular issues under Rule 42(d)(l) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants failed to timely notify the public of the Data Breach;

b. Whether Defendants owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendants' security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendants failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

162. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION AND CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiffs and the Class)

163. Plaintiffs re-alleges and incorporates by reference paragraphs 1–162, as if fully set forth herein.

164. By collecting and storing the Private Information of Plaintiffs and Class Members, in their computer system and network, and sharing it and using it for commercial gain, Defendants owed a duty of care to use reasonable means to secure and safeguard their computer systems—and Class Members' Private Information held within them —to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duties included a responsibility to implement processes by which they could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

165. Defendants owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed

herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

166. Plaintiffs and Class Members are a well-defined, foreseeable, and probable group of patients that Defendant was aware of, or should have been aware, could be injured by inadequate data security measures.

167. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant GH and its information technology vendor Defendant Nuance, on the one hand, and Defendant GH and its patients, on the other hand, which is recognized by laws and regulations including but not limited to HIPAA, the FTC Act, and common law. Defendants were in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

168. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

169. In addition, Defendants had a duty to employ reasonable security measures

under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

170. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

171. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to ensure that their email system had plans in place to maintain

reasonable data security safeguards;

d. Failing to have in place appropriate mitigation policies and

procedures;

e. Allowing unauthorized access to Class Members' Private Information;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

172. Plaintiffs and Class Members have no ability to protect their Private Information that was or remains in Defendants' possession.

173. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

174. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members. In addition, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

175. Defendants' conduct was grossly negligent and departed from reasonable standards of care, including but not limited to, failing to adequately protect the

Private Information, and failing to provide Plaintiffs and Class Members with timely notice that their sensitive Private Information had been compromised.

176. Neither Plaintiffs nor Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

177. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

178. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendants' breaches of their duties. Defendants knew or should have known that they were failing to meet their duties, and that Defendants' breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the theft and exposure of their Private Information.

179. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, nominal, and other damages as appropriate and ordered by the Court in an amount to be proven at trial.

SECOND CAUSE OF ACTION AND CLAIM FOR RELIEF
Negligence *Per Se*
(*On behalf of the Plaintiffs and the Class*)

180. Plaintiffs incorporate by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 162, as if set forth fully herein.

181. Section 5 of the FTC Act, 15 U.S.C. 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendants of failing to use reasonable measures to protect Plaintiffs' and Class members' Private Information. Various FTC publications and orders also form the basis of Defendants' duty.

182. Defendants violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiffs' and Class members' Private Information and not complying with industry standards.

183. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendants' systems.

184. Defendants' violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se.*

185. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

186. Moreover, the harm that has occurred is the type of harm the FTC Act (and

similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class members.

187. As a result of Defendants' negligence, Plaintiffs and the other Class members have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

THIRD CAUSE OF ACTION AND CLAIM FOR RELIEF
Breach of Implied Contract
(*On behalf of the Plaintiffs and the Class*)

188. Plaintiffs re-alleges and incorporates by reference paragraphs 1-162, as if set forth fully herein.

189. Defendants acquired and maintained the Private Information of Plaintiffs and the Class.

190. Plaintiffs and the Class were required to deliver their Private Information to Defendants as part of the process of obtaining services provided by Defendants.

Plaintiffs and Class Members paid money, or money was paid on their behalf, to Defendants in exchange for services.

191. Defendants solicited, offered, and invited Class Members to provide their Private Information as part of their regular business practices. Plaintiffs and Class Members accepted Defendants' offers and provided their Private Information to Defendants, or, alternatively, provided Plaintiffs' and Class Members' information to doctors or other healthcare professionals, who then provided the Private Information to Defendants.

192. Defendants accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services to Plaintiffs and Class Members.

193. In accepting such information and payment for services, Defendants entered into an implied contract with Plaintiffs and the other Class Members whereby Defendants became obligated to reasonably safeguard Plaintiffs' and the other Class Members' Private Information.

194. Alternatively, Plaintiffs and Class Members were the intended beneficiaries of data protection agreements entered into between Defendants and subsidiary healthcare providers.

195. In delivering their Private Information to Defendant and paying for healthcare services, Plaintiffs and Class Members intended and understood that Defendants would adequately safeguard their data as part of that service.

196. The implied promise of confidentiality includes consideration beyond those pre- existing general duties owed under HIPAA or other state or federal statutes and regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

197. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of their agents is restricted and limited to achieve only authorized medical purposes; (3) restricting data access only to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

198. Plaintiffs and the Class Members would not have entrusted their Private Information to Defendants in the absence of such an implied contract.

199. Had Defendants disclosed to Plaintiffs and the Class (or their physicians or other healthcare professionals) that they did not have adequate computer systems and security practices to secure sensitive data and Private information, Plaintiffs and the other Class Members would not have provided their Private Information to

Defendants (or their physicians or other healthcare professionals to provide to Defendants).

200. Defendants recognized that Plaintiffs' and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and the other Class Members.

201. Plaintiffs and the other Class Members fully performed their obligations under the implied contracts with Defendants.

202. Defendants breached the implied contract with Plaintiffs and the other Class Members by failing to take reasonable measures to safeguard their Private Information as described herein.

203. As a direct and proximate result of Defendants' conduct, Plaintiffs and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

FOURTH CAUSE OF ACTION AND CLAIM FOR RELIEF
Unjust Enrichment
(*On Behalf of Plaintiffs and the Class*)

204. Plaintiffs re-alleges and incorporates by reference paragraphs 1–162, as if set forth fully herein.

205. This count for Unjust Enrichment is pleaded in the alternative to any breach

of contract claim.

206. Upon information and belief, Defendants pay for data security measures entirely from general revenue, including from money they make based upon protecting Plaintiffs' and Class Members' Private Information.

207. There is a direct nexus between money paid to Defendants and the requirement that Defendants keep Plaintiffs' and Class Members' Private Information confidential and protected.

208. Plaintiffs and Class Members paid Defendants and/or healthcare providers a certain sum of money, which was used to fund data security via contracts with Defendants.

209. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

210. Protecting data from Plaintiffs and the rest of the Class Members is integral to Defendants' businesses. Without Class Members' data, Defendant Geisinger would not be able to provide healthcare services and Defendant Nuance would not be able to provide information technology services to Geisinger, thus compromising both of Defendants' core businesses.

211. Plaintiffs' and Class Members' data has monetary value, and Plaintiffs and

Class Members directly and indirectly conferred a monetary benefit on the Defendants. They indirectly conferred a monetary benefit on Defendants by purchasing goods and/or services from entities that contracted with Defendants, and from which Defendants received compensation to protect certain data. Plaintiffs and Class Members directly conferred a monetary benefit on Defendants by supplying Private Information, which has monetary value, from which value Defendants derive their business values, and which should have been protected with adequate data security.

212. Defendants knew that Plaintiffs and Class Members conferred a benefit which Defendants accepted. Defendants both profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

213. Defendants enriched themselves by saving the costs they reasonably should have expended on adequate and reliable data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to avoid their data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

214. Under the principles of equity and good conscience, Defendants should not

be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendants failed to implement and pay for appropriate data management and security measures that are mandated by industry standards.

215. Defendants acquired the monetary benefit and Private Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

216. If Plaintiffs and Class Members knew that Defendants had not secured their Private Information, they would not have agreed to provide their Private Information to Defendants.

217. Plaintiffs and Class Members have no adequate remedy at law.

218. As a direct and proximate result of Defendants' wrongful conduct, Plaintiffs and Class Members have suffered and will continue to suffer injury, including but not limited to:

(i) actual identity theft;

(ii) the loss of the opportunity to determine how their Private Information is used;

(iii) the compromise, publication, and/or theft of their Private Information;

(iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use

of their Private Information;

(v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft;

(vi) the continued exposure risk to their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Private Information in their continued possession;

(vii) loss or privacy from the unauthorized access and exfiltration of their Private Information; and

(viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

219. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

220. Defendants should be compelled to disgorge into a common fund or

constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendants' services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiffs Mark Dushok, A.F. and G.G-F., and Christina Izquierdo as Class Representatives and their counsel as Class Counsel;

b) For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

c) For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendants to pay for not less than five years of credit

monitoring and identify theft services for Plaintiffs and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, nominal damages, statutory penalties, and other damages the Court deems appropriate, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) Pre- and post-judgment interest on any amounts awarded; and,

i) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of any and all issues in this action so triable as of right.

Dated: July 31, 2024

Respectfully Submitted,

/s/Kelly Iverson
Kelly Iverson, Esq.

Gary F. Lynch, Esq. (PA 56887)
Kelly Iverson, Esq. (PA 307175)
LYNCH CARPENTER
1133 Penn Avenue, 5th Fl.
Pittsburgh, PA 15222
Tel: 412 322.9243
gary@lcllp.com
kelly@lcllp.com

Ariana J. Tadler, Esq.*
TADLER LAW LLP
22 Bayview Avenue, Suite 200
Manhasset, NY 11030
Tel: 212.946.9300

atadler@tadlerlaw.com

A.J. de Bartolomeo, Esq.*
TADLER LAW LLP
P.O. Box 475847
3749 Buchanan Street
San Francisco, CA 94123
Tel: 415.226.0260
ajd@tadlerlaw.com

Marion Munley, Esq. (PA 46957)
MUNLEY LAW PC
227 Penn Avenue
Scranton, PA 18503
Tel: 570.346.7401
mmunley@munley.com

* *Pro Hac Vice Forthcoming*

Counsel for Plaintiffs